

## CLAIMS

1. A method for securing network-connected resources,  
the method comprising:
  - 5 at a first network-connected node, receiving an electronically formatted job;
  - receiving CK, a symmetrical encryption key (K) encrypted using an asymmetrical encryption public key (pubK);
  - receiving CH, a hash (H) of the job, further encrypted using
  - 10 K;
  - decrypting CK using an asymmetrical encryption private key (privK), corresponding to pubK, to recover K;
  - hashing the job, generating H';
  - using K to validate CH;
  - 15 in response to validating CH, decrypting an encrypted resource using K; and,
  - using the decrypted resource to process the job.
2. The method of claim 1 wherein using K to validate CH
- 20 includes:
  - encrypting H' using K, obtaining CH'; and,
  - matching CH to CH'.
3. The method of claim 1 wherein using K to validate CH
- 25 includes:
  - decrypting CH using K, generating H; and,

comparing H to H'.

4. The method of claim 1 further comprising:  
prior to receiving the job, CK, and CH, receiving the  
5 encrypted resource; and,  
storing the encrypted resource.

5. The method of claim 4 further comprising:  
installing pubK,privK upon initialization.

10

6. The method of claim 1 wherein receiving an  
electronically formatted job includes receiving a print job in a format  
selected from the group including text and image formats.

15 7. The method of claim 4 wherein storing the encrypted  
resource includes storing an encrypted font resource; and,  
wherein using the decrypted resource to process the job  
includes printing a print job using the decrypted fonts.

20 8. The method of claim 7 wherein storing the encrypted  
font resource includes storing resources selected from the group including  
a logo, personal signature image, and glyph.

9. The method of claim 4 wherein receiving the encrypted  
25 resource includes receiving the encrypted resource in a format selected

from the group including hypertext transport protocol (http) and file transport protocol (FTP).

10. The method of claim 1 further comprising:  
5 at a second network-connected node, generating the job;  
encrypting K with pubK, generating CK;  
hashing the job, generating H;  
encrypting H using K, generating CH; and,  
sending the job, CK, and CH to the first node for job  
10 processing.

11. The method of claim 1 further comprising:  
receiving a selection command for a particular one of a  
plurality of encrypted resources; and,  
15 wherein decrypting an encrypted resource using K, in  
response to a valid match, includes decrypting the selected resource.

12. The method of claim 11 wherein receiving a selection  
command for a particular one of a plurality of encrypted resources  
20 includes receiving  $CK_i$ , where  $1 \leq i \leq m$ ; and,  
wherein decrypting the selected resource in response to the  
encrypted resource selection command includes decrypting  $CK_i$  to recover  
one of symmetrical encryption keys  $K_1$  through  $K_m$ , where  $K_1$  through  $K_m$   
correspond to encrypted resources  $CR_1$  through  $CR_m$ .

25

13. The method of claim 1 wherein receiving an electronically formatted job includes receiving the job at network-connected node  $N_i$ , where  $1 \leq i \leq n$ ;

wherein receiving CK includes  $N_i$  receiving  $CK_i$ , where  $CK_i$  is  
5 generated by encrypting K using corresponding asymmetrical encryption public key  $pubK_i$ ; and,

wherein decrypting CK includes  $N_i$  decrypting  $CK_i$  using corresponding asymmetrical encryption private key  $privK_i$ , to recover K.

10 14. The method of claim 1 wherein receiving an electronically formatted job includes receiving the job at network-connected node  $N_i$ , where  $1 \leq i \leq n$ ;

wherein receiving CK includes  $N_i$  receiving  $CK_i$ ,  
corresponding to symmetrical encryption key  $K_i$ , encrypted using  $pubK_i$ ;

15 wherein receiving CH includes  $N_i$  receiving  $CH_i$ , a hash of the job encrypted using corresponding symmetrical encryption key  $K_i$ ;  
and,

wherein decrypting CK includes  $N_i$  decrypting  $CK_i$  using  
asymmetrical encryption private key  $privK_i$ , to recover corresponding  
20 symmetrical encryption key  $K_i$ .

15. The method of claim 14 wherein using K to validate CH includes:

$N_i$  encrypting H' using symmetrical encryption key  $K_i$ ,  
25 obtaining  $CH_i'$ ;

$N_i$  matching  $CH_i$  to corresponding  $CH_i'$ ; and,

wherein decrypting an encrypted resource using K includes  
N<sub>i</sub> decrypting the encrypted resource using symmetrical encryption key  
K<sub>i</sub>.

5                    16.    The method of claim 14 wherein using K to validate  
CH includes:

N<sub>i</sub> decrypting CH<sub>i</sub> using symmetrical encryption key K<sub>i</sub>,  
obtaining H;

N<sub>i</sub> comparing H to H'; and,

10                    wherein decrypting an encrypted resource using K includes  
N<sub>i</sub> decrypting the encrypted resource using symmetrical encryption key  
K<sub>i</sub>.

15                    17.    A method for accessing network-connected processing  
resources, the method comprising:

at a second node, generating an electronically formatted job;  
encrypting a symmetrical encryption key K with an  
asymmetrical encryption key (pubK), generating CK;

20                    hashing the job generating H;  
encrypting H using K, generating CH;  
sending the job, CK, and CH to a first network-connected  
node; and,

processing the job at the first node using a K encrypted  
resource.

25

18. A system for using secure network-connected resources, the system comprising:

a first device including:

5 a network-connected port for receiving an electronically formatted job, for receiving CK, a symmetrical encryption key (K) encrypted using an asymmetrical encryption public key (pubK), and for receiving CH, a hash (H) of the job, further encrypted using K;

10 a hash unit having an interface to accept the job and to supply a hash of the job (H');

a memory having an interface to supply an asymmetrical encryption private key (privK), corresponding to pubK, and an encrypted resource;

15 a security unit having an interface to authorize access to the encrypted resource in memory, in response to validating CH; and,

a processing unit having an interface to accept the job and a decrypted resource, and to supply a job processed using the decrypted resource.

20

19. The system of claim 18 further comprising:

a decrypting unit having an interface to accept CK and privK, to generate K in response to decrypting CK using privK, to decrypt the encrypted resource from memory using K, and  
25 supply the decrypted resource;

an encryption unit having an interface to accept H' and K, and supply CH' in response to using K to encrypt H'; and, wherein the security unit accepts CH and CH' and validates CH by matching CH to CH'.

5

20. The system of claim 18 further comprising:

a decrypting unit having an interface to accept CH, CK, and privK, to generate K in response to decrypting CK using privK, to supply H in response to decrypting CH using K, and

10

supply the decrypted resource; and, wherein the security unit accepts H and H' and validates CH by matching H to H'.

21. The system of claim 18 wherein the network-connected port receives the encrypted resource for storage in the memory.

15

22. The system of claim 18 wherein the memory is a read only memory (ROM) for accepting and storing privK upon device initialization.

20

23. The system of claim 18 wherein the first device is a printer; and,

wherein the network-connected port receives a print job in a format selected from the group including text and image formats.

25

24. The system of claim 23 wherein the memory stores encrypted font resources; and,  
wherein the processing unit is a print engine that supplies a job printed using the decrypted fonts.

5

25. The system of claim 24 wherein the memory stores encrypted font resources selected from the group including a logo, personal signature image, and glyph.

10 26. The system of claim 21 wherein the network-connected port receives an encrypted resource for storage in a format selected from the group including hypertext transport protocol (http) and file transport protocol (FTP).

15 27. The system of claim 18 further comprising:  
a second device including:  
a processor to supply a job;  
a hash unit having an interface to accept the job  
and to supply a hash of the job (H);  
20 an encryption unit having an interface to accept H, to supply CK, the encryption of symmetrical encryption key K using pubK, and CH, the encryption of H using K; and,  
a network-connected port for transmitting the  
job, CK, and CH to the first device for job processing.

25



28. The system of claim 18 wherein the first device network-connected port receives a encrypted resource selection command; and,

wherein the decryption unit decrypts the selected resource.

5

29. The system of claim 28 wherein the decryption unit decrypts  $CK_i$ , where  $1 \leq i \leq m$ , to recover one of symmetrical encryption keys  $K_1$  through  $K_m$ , where  $K_1$  through  $K_m$  correspond to encrypted resources  $CR_1$  through  $CR_m$ .

10

30. The system of claim 18 further comprising:

a plurality of devices  $N_i$ , where  $1 \leq i \leq n$ , each receiving the electronically formatted job at a network-connected port, along with  $CK_i$ , where  $CK_i$  is generated by encrypting  $K$  using corresponding

15 asymmetrical encryption public key  $pubK_i$ ; and,

wherein each device decryption unit decrypts  $CK_i$  using corresponding asymmetrical encryption private key  $privK_i$ , to recover  $K$ .

31. The method of claim 18 further comprising:

20 a plurality of devices  $N_i$ , where  $1 \leq i \leq n$ , each receiving the electronically formatted job at a network-connected port, along with  $CK_i$ , where  $CK_i$  is generated by encrypting  $K_i$  using corresponding asymmetrical encryption public key  $pubK_i$ , and  $CH_i$ , a hash of the job encrypted using corresponding symmetrical encryption key  $K_i$ ; and,

25 wherein each device includes a decryption unit for decrypting  $CK_i$  using asymmetrical encryption private key  $privK_i$ , to recover

corresponding symmetrical encryption key  $K_i$ , for the decryption of the encrypted resource.

32. The system of claim 31 wherein each device encryption  
5 unit encrypts  $H'$  using symmetrical encryption key  $K_i$ , obtaining  $CH_i'$ ;  
and,

wherein each device security unit validates  $CH$  by matching  
 $CH_i$  to corresponding  $CH_i'$ .

10 33. The system of claim 31 wherein each device decryption  
unit decrypts  $CH_i$  using symmetrical encryption key  $K_i$ , obtaining  $H_i$ ; and,  
wherein each device security unit validates  $CH$  by matching  
 $H$  to  $H'$ .

15 34. A system for accessing network-connected processing  
resources, the system comprising:

a second device including:

a processor to supply a job;

a hash unit having an interface to accept the job

20 and to supply a hash of the job ( $H$ );

an encryption unit having an interface to accept  
 $H$ , to supply  $CK$ , the encryption of symmetrical encryption key  $K$   
using  $pubK$ , and  $CH$ , the encryption of  $H$  using  $K$ ; and,

25 a network-connected port for transmitting the  
job,  $CK$ , and  $CH$  to a first device for job processing.